

# Enabling Army Digital Organizations

---

06 July 2010

MAJ Darrell Collins  
Brigade Operations Research/System Analyst  
darrell.collins@us.army.mil

Significant Contributors include:

MAJ Michael Gephart, Brigade Knowledge Manager and Chief of Fusion;  
CW3 Kevin Gonzales, Brigade Network Operations Technician;  
Dr. Brenda Wenzel, Director, Training Analysis Division;  
MAJ Anne-Marie Wiersgalla, Brigade Signal Officer;  
CPT Chris Alexander, Assistant Signal Officer;  
Ms. Sara Krondak, Training Analyst.

Reviewers include:

MSG Richard Lang, Brigade Signal NCO;  
MAJ Eric Haas, Brigade HUMINT Coordinator;  
MAJ Derek McClain, Brigade Intelligence Officer;  
CPT Sunny Chen, Brigade Intelligence Planning Officer;  
CPT Richard Richardson, Brigade Assistant Intelligence Officer.

Assigned to the TRADOC Analysis Center – White Sands Missile Range, MAJ Darrell Collins deployed to Kandahar, Afghanistan as an Operations Research/System Analyst (ORSA) in October 2009 to support the 5<sup>th</sup> Brigade, 2<sup>nd</sup> Infantry Division, a Stryker Brigade Combat Team [5/2 ID (SBCT)] under the Brigade/Regiment Combat Team (BCT/RCT) ORSA program. The Joint Improvised Explosive Device Defeat Organization (JIEDDO) sponsors this program, which provides Operations Research analysts to work directly for deployed Brigade Commanders to assist with quantitative and qualitative analysis throughout the decision-making process, allocation of scarce resources, and assessments of operations. MAJ Collins and LTC(ret.) Thomas Schwartz provided trend analysis and forecasting of operational and significant activities, route discipline analysis and assistance using Blue Force Tracker Honesty Traces, campaign assessment support from the battalion to the regional command level, and analytical and technical assistance to the staff.

Report Documentation Page			Form Approved OMB No. 0704-0188		
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE <b>06 JUL 2010</b>		2. REPORT TYPE		3. DATES COVERED <b>00-00-2010 to 00-00-2010</b>	
4. TITLE AND SUBTITLE <b>Enabling Army Digital Organizations</b>			5a. CONTRACT NUMBER		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S)			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>Department of the Army, Washington, DC, 20301</b>			8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)			10. SPONSOR/MONITOR'S ACRONYM(S)		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release; distribution unlimited</b>					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT <b>Same as Report (SAR)</b>	18. NUMBER OF PAGES <b>18</b>	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>			

## Enabling Army Digital Organizations

The “rapid pace of technology” is an oft-used phrase applied to many areas, but the changes in data processing and visualization applications combined with the increased exposure of Soldiers to flexible data exchange formats and high level scripting languages has significant implications on the Army’s Digital Education and infrastructure. During the deployment of the 5<sup>th</sup> Brigade, 2<sup>nd</sup> Infantry Division, a Stryker Brigade Combat Team [5/2 ID (SBCT)], there were several insights developed about the current state of “Army Digital Education.” Three of these insights (education, experience, and flexibility) act together in their influence on the effectiveness of the unit in employing the Army Battle Command Systems (ABCS). Although important in their own right, the interrelation of education, experience, and flexibility has a significant impact on the formation and development of a “digital organization.” The underlying theme connecting them in this context is that as data exchange capabilities and technology evolves at a rapid pace, the Army must examine the training, employment, and digital infrastructure to ensure that the programs and policies enable Soldiers and Leaders and to encourage vision and innovation at the lowest level.

*The current state of institutional “digital education” and lack of “hands-on” experience limit the ability of incoming Soldiers to use the Army Battle Command Systems (ABCS) and inhibits the incoming leaders’ understanding of what is possible and how to best incorporate them into his or her vision for operations, resulting in an unnecessary learning curve in the deployed unit’s ability to process data and lost opportunities to adapt the systems to a particular tactical or operational problem.*

*Similarly, “consolidation of servers” at the Directorate of Information Management (DOIM) level significantly limits the unit’s administrators’ “hands-on” experience and currency with rapidly changing patches, restrictions, and other compliance requirements which significantly impairs the security, quality of service, and flexibility of the deployed unit’s digital infrastructure.*

*Finally, while the Publish And Subscribe Server (PASS), United States Message Text Format (USMTF), Variable Message Format (VMF), and other standards provide a solid base, the incorporation of accredited client applications to provide “safe” client access to the ABCS server data through common data exchange primitives in flexible information exchange formats combined with a holistic architecture review should enable units to explore more customization and innovation and the ability to provide tailored SA as well as incorporate new technologies and applications without the need to rely on CONUS based software engineers.*

## Balancing acts

Like all training and doctrine efforts, each topic this whitepaper will address is actually a balancing act between two mutually desired, but generally exclusive purposes and ideals. These trade-off decisions imply that no one solution is “correct” and even the best solution for now is likely to be “wrong” in the near future. Thus, the most appropriate path forward is not to “train Soldiers,” or “build system

## Enabling Army Digital Organizations

requirements” but to *enable* Soldiers and lay down *data exchange foundations*. The discussion of some of these “balancing acts” will follow the discussion of the three main points.

### Enabling

It is important to note that for this whitepaper, digital system training is only one component of enabling, and it is not necessarily the current limiting factor, especially with the collective administrative tasks.

Various individuals from across the acquisition community, Training and Doctrine Command (TRADOC), and Forces Command (FORSCOM) units have espoused the concept of employing the battle command systems on a daily basis in garrison. The Brigade Commander, COL Tunnell, disagrees and likens Army Digital Education to weapons training. Soldiers do not carry personal weapons on a daily basis. The training generally occurs with the M16, Soldiers are then fully capable of employing any M16-variant with only minor adjustments to the handling and ballistic characteristics while deployed. However, other than the procedures to load, clear, and disassemble the M16 (and variants), the training is really about the process of marksmanship.

All forms of training must balance time and resources between processes and procedures. Processes encompass the responsibilities and duties of the battlefield or staff function in concepts and objectives similar to mission statements (Who, What, Where, When, and Why), where procedures are tightly focused on the How. Emphasizing process over procedure may lead to generating students who know what they are to do and why, but completely unprepared in how to actually do it. Emphasizing procedure over process conversely may lead to students who are adept at how to do things without a solid understanding of why or when they should do them.

Similarly, enabling Soldiers at the user level means more than training them on the systems. The first part of enabling Soldiers means giving them a solid foundation on the digital processes equivalent to Military Operational Specialty (MOS) training on their functional processes: i.e. what they are actually trying to accomplish, why they should Process, Exploit, and Disseminate (PED) data this way, and how their input data and processing interacts with other users. The second part of enabling is to combine procedural training with enough hands-on experience in making the systems work together to produce Soldiers who are confident and comfortable enough to employ the systems and data in new and unique ways to accomplish any mission. Numerous leaders and Soldiers are “trained” on Microsoft Word™, but most do not understand or employ paragraph styles and section formatting techniques to build processes that ease and standardize daily tasks and products.

Perhaps the best explanation may be that you *train* Soldiers and Leaders to accomplish the tasks necessary to employ the systems together as designed, whereas you *enable* them by developing the robust knowledge and skills required to employ the systems in new and innovative ways.

### How do we enable users?

Stryker brigades are equipped with a significant digital infrastructure, and as an organizational goal, the Soldiers and Leaders of the 5/2 ID (SBCT) strived to exploit the fielded systems fully and to incorporate new systems and technologies. A few examples include:

- CPT Jared Cox, the Assistant Fire Support Officer supervised the integration of the Enhanced Position Locating and Reporting System (EPLRS) on the unit's vehicles and dismounted LandWarrior systems with the Situation Awareness DataLink (SADL) on fighter and other aircraft to assist Close Air Support pilots in locating and communicating with the ground forces.
- The S-2 section and MI Company with MAJ Derek McClain, CPT Michelson, CW2 Earl Wilson III, et al., built intelligence processes and procedures to maximize the utilization of the Distributed Common Ground System – Army (DCGS-A) – moving well past that of any previous use or testing; consequently providing crucial feedback as they encountered and worked through undiscovered bugs and problems with the Program Manager.
- The brigade studied a Purdue University project called the Local Decision-Maker™, which applied geospatial visualization and analysis toolsets to various data layers to inform decisions. CW2 Todd Grabinski created the Stryker ASCOPE (Areas, Structures, Capabilities, Organizations, People, and Events) Decision-Maker, a similar capability using the Digital Topographic Support System (DTSS) which was linked into the DCGS-A ArcSDE (Spatial Database Engine)™.
- The brigade expanded the use of Google Earth™ as a dynamic visualization and briefing tool over static PowerPoint™ slides, with the ability to drill directly into the same databases used by DCGS-A and the Stryker ASCOPE Decision-Maker.
- The brigade also spearheaded the use of Palantir™ to enable functions similar to DCGS-A below battalion level in the Company Intelligence Support Teams (COIST).

In order to achieve these goals, the brigade dedicated a lot of time and effort to allow the Soldiers and Leaders to gain the right knowledge and experience with the equipment and internalize the basics of Information and Knowledge Management. Although time extremely well spent, the establishment of this foundation of individual skills and knowledge competed for the limited training time with collective tasks and collaborative skills. Consequently, around the 3/4 mark of the deployment - after the Soldiers and Leaders had refined their processes and procedures in combat operations, the Brigade Commander asked the Brigade Signal Officer, MAJ Anne-Marie Wiersgalla, to create a survey to examine how well the institutional and home-station training prepared the Soldiers to use digital systems. MAJ Wiersgalla, MAJ Michael Gephart, the Brigade Knowledge Manager, and CPT Chris Alexander, the Assistant Signal Officer, developed and collected the survey through the brigade SharePoint™ portal. They asked MAJ Darrell Collins, the Brigade Operations Research/Systems Analyst, for assistance with analyzing the results who enlisted reach-back support from Dr. Brenda Wenzel and Ms. Sara Krondak, Engineering Psychologists in the Training Analysis Division of the TRADOC Analysis Center – White Sands Missile Range.

## Enabling Army Digital Organizations

### Survey Results

The survey captured the responses from 36 Officers (10 Field Grade and 26 Company Grade), 29 Non-Commissioned Officers (NCO) (17 Senior NCO, 12 Junior NCO), and four Specialists. The responses covered three echelons (45 at company, 19 at battalion, 5 at brigade) and 9 duty positions (platoon leaders and platoon sergeants, company intelligence support teams, operations NCO, company commanders and first sergeants, battle captains and NCO, battalion and brigade staff). The respondents had been in their positions for a collective 964 months, although 57% were in position less than one year. The survey questions included prior and existing knowledge, use, and training related to digital systems in general. The survey also included specific questions on five systems: the Force XXI Battle Command Brigade and Below (FBCB2) system employed with both satellite (Blue Force Tracker (BFT)) and terrestrial (EPLRS) radios; the Tactical Ground Reporting System (TIGR); the Command Post of the Future (CPOF); and the Maneuver Control System (MCS).

### General Knowledge

Forty-eight percent of the respondents assessed themselves as at least familiar with digital systems in general, and another 20% indicated specialized knowledge related to the systems they primarily use. The responses to questions on which systems the respondent used and how often, the FBCB2-BFT system was the most used system across all echelons, followed by CPOF, FBCB2-EPLRS, TIGR, and MCS.

Respondents were asked to assess their ability to maintain and troubleshoot these systems plus a Voice Over Internet Protocol (VOIP) telephone and a standard laptop/desktop computer, and to identify the correct first troubleshooting step from a multiple-choice quiz. Granting credit for selecting either of the first two troubleshooting steps, the quiz generally supported the self-assessments, except for the FBCB2-EPLRS, where just over one-half of those professing maintenance skills marked one of the two steps. These results were also generally consistent with the number of respondents who indicated they used a system more than “some of the time.”

Overall, around half of the respondents self-assessed themselves as familiar with the systems in general, and a similar percentage with maintaining the systems when backed up with the quiz. It is clear that Soldiers need more training to become self-sufficient at maintaining and troubleshooting these systems.

### Training Assessments

Respondents assessed both their current level of knowledge on Army Battle Command Systems, and their level when they first took their job. Overall, 33% of the 69 respondents assessed themselves as currently proficient, up from the 9% who indicated incoming proficiency. Nine percent assessed themselves as initially untrained, but currently proficient. Five respondents indicated some loss of proficiency, although two are now Company Commanders and there may have been some confusion between the “Trained” and “Adequate” ratings.

The NCO and Soldiers rated the amount of training they received on the five systems during five professional development schools: 32 from Basic Training (BT); 31 from Advanced Individual Training (AIT); 28 from the Primary Leader Development Course (PLDC); 24 from the Basic NCO Course (BNCOC); and 19 from the Advanced NCO Course (ANCOC). Collectively, only 13% of the responses indicated that

## Enabling Army Digital Organizations

the digital training from institutional schools prepared them for their positions. Likewise, just 1% of the combined 670 responses indicated institutional schools provided above-average digital system training, whereas 95% reported no institutional training on the surveyed systems.

The officers rated their training on the systems during three professional development schools: 33 from the Officer Basic Course (OBC), 24 from the Captain's Career Course (CCC), and 8 from Intermediate Level Education (ILE). Their responses were slightly higher, with 33% of the responses indicating that the digital training prepared them for their positions. Their assessment of the training suggests that more digital training occurred in the officer schools, as only 77% of the 330 responses reported no institutional training, although merely 5% rated any of it as above-average.

In contrast, for home-station and CTC training, 72% of the NCO and Soldier responses indicated that it prepared them for their current position, five times the response rate for institutional school training. The officer responses, slightly lower at 61%, were double the rate for institutional school training. The assessment of the training was similar between the groups, with 17% of the 309 NCO and Soldier responses and 15% of the 320 officer responses indicating above-average ratings, with 55% and 50% respectively reporting no digital training. This suggests a different focus on digital training between the NCO and officer professional development schools.

Collectively, the survey clearly demonstrated that, although the Soldiers are learning how to use digital systems on-the-job, it is not sufficient to close the perceived training and proficiency gap. Moreover, even with the competition for limited training time, home-station training and Combat Training Center (CTC) experiences better prepared the Soldiers for the employment of digital systems than did institutional training. The Army needs to provide digital system training consistently throughout the Soldiers' Professional Military Education.

### Digital Culture

The success or failure in moving from training to enabling lies in the creation and adoption of a "digital culture,"<sup>1</sup> which in the future technological world, is no less important than the Army Values, Soldier's Creed, and Warrior Ethos. The Army Knowledge Management (AKM)<sup>2</sup> strategy acknowledged the need for a cultural shift in the Information Technology (IT) arena in 2001-2002, with the call for *"the Army to change its cultural thinking from the 'islands of automation' mentality to the Enterprise management of IT resources. This means that organizational IT investments must support the Army's Enterprise-wide goals under AKM."* Now the Army needs to institute a similar cultural change in the training and development of Soldiers and Leaders.

Although almost every member of the staff employs numerous digital systems and applications on a daily basis, informal interviews indicated that almost every officer school still uses paper maps and acetate overlays. Static PowerPoint™ slideshows were the only apparent automation, which, for the purpose of visualization and information exchange, are little different from ViewGraphs, although easier to distribute, and arguably, produce. PowerPoint™ was a huge advance from overhead projectors, ViewGraphs, and water-based markers – in 1997. Thirteen years later, the standard remains static overhead briefing charts, albeit delivered over collaborative tools such as Adobe Connect™.

## Enabling Army Digital Organizations

Creating a digital culture requires more than simply upgrading to the current software version just to recreate 1960's era overhead slides. In order to appreciate and exploit them, Soldiers and especially Leaders will have to understand the visualization and dynamic content generation capabilities of ArcGIS™, Google Earth™, and other tools. Similarly, to streamline reporting and improve situational awareness, they need to understand the collaborative processing capabilities of dashboards, business data catalogs, and reporting services in Microsoft Office SharePoint Server™ and similar groupware.

The real beneficiaries of the improved collaborative reporting capabilities are the Soldiers and NCOs on the staff. Battle-staff NCOs and Operations SGMs are the heart of the Tactical Operations Center, and in digital organizations, they need to be just as technically proficient in the areas of Information and Knowledge Management as they are with radios, maps, and tracking boards. With the exception of the Knowledge Management Officer (KMO), their training and proficiency on digital systems is probably more critical to maintaining a highly functioning digital organization than any of the other officers.

Given that NCOs reported the least amount of digital training, and their critical role in establishing and running the organization, the greatest challenge for a digital organization is to establish that base of knowledge within the NCO corps. That is not to say that NCOs should now forego their traditional leadership, supervisory, and combat skills, just that the current institutional schools are not providing the base digital education and skill sets needed to support digital organizations. The Army needs to invest in Information and Knowledge Management training, carefully balancing it with the leadership and combat skill training required for their leadership positions, and the changes must begin in the institutional training programs.

### Institutional Training

Current institutional training generally focuses on single systems. With some exceptions, task based training on single systems limits the Soldier's experience with the complex interactions and interdependencies of the entire ABCS suite. In addition, it likely focuses on current digital processes (the conceptual thread connecting several procedures with an identifiable end-state) and digital procedures (the specific steps to accomplish each task) and does not address how to monitor and potentially exploit and fuse data from other sections or Military Occupational Specialties (MOS).

Both the survey and informal interviews suggest that, coming into the deployment, Soldiers gained most of their ABCS knowledge during home-station training. With the bulk of training time occurring at home-station, the current model of training ~30% of all the required skills in Basic Training / Advanced Individual Training and leaving the rest as unit training may be necessary; however, digital home-station training could be better spent on integrating the battle command systems into functioning unit processes than simply learning how to use them.

### Tactics, Techniques, and Procedures

Examining the Tactics, Techniques, and Procedures (TTP) construct in reverse, the Soldiers should be thoroughly versed on Procedures (how to make it work) before moving on to Techniques (how to make it work - under \_x\_ conditions), otherwise training designed to teach a technique is hampered by attention diverted to accomplish the subordinate procedures.



## Enabling Army Digital Organizations

In the previous marksmanship analogy, the Procedures generally equate to individual skills such as the Four Fundamentals of Marksmanship (Steady Hold, Aiming, Breath Control, and Trigger Squeeze) or Immediate Action drills such as Slap, Pull, Observe, Release, Tap, and Shoot (SPORTS). Digital equivalents may include creating and processing a combat report, querying a database of these reports, selecting optimal key words in those queries, or the Immediate Action drill for a non-responding application. Although generally constructed as part of the system during fielding, the Army should carefully review these procedural level tasks to ensure they support and integrate with the fundamentals of the Soldiers' particular duties, and do not become rote system-specific tasks and workflows based on the current version of the program or application.

However, practice and rote "muscle-memory" are an important part of the process; familiarity with the procedures is not sufficient. Recent research suggests that the difference between high performing and average athletes is the amount of their "attention" allocated to performing physical movements such as catching a ball. The higher performing athletes need to employ relatively less of their attention to catch the ball, leaving more attention for applying toward other aspects such as situational awareness or strategy. This seems to compare directly to Soldiers' mastery of Procedures: these are the critical skills, which if not mastered, will draw attention and detract from later training on Techniques.

Just as the Army teaches techniques like marksmanship under various conditions, such as limited visibility, so should it incorporate operations under equivalent digital conditions such as limited bandwidth. The multitude of potential conditions hampers any attempt to incorporate them all, but simply selecting a set of common conditions falls short of the desired objective. The Army should first focus on thoroughly covering the information architecture, and only then select the most-likely conditions to exercise the problem-solving process. By shifting the focus toward the capabilities, interactions, and most importantly the purposes behind the systems and infrastructure, instructors can present the conditions-based training as a critical thinking or puzzle-solving problem instead of simple responses to specific conditions. It is important not to limit the conditions to physical or technical aspects, as differing task organizations, styles, priorities, and operational goals may call for very different Techniques and Tactics.

Like the transition from Procedures to Techniques, Soldiers usually need to be skilled at both levels before they have the foundation to get really creative with the Tactics (how to make it work - under \_x\_ conditions - to accomplish \_y\_ mission). Following logically, maximizing the Soldiers' and units' collective training time requires Institutional Training programs to produce Soldiers thoroughly versed on the Procedures and competent at employing and adapting Techniques to the situation, so that the bulk of the unit's time can occur at the Tactics level.

In the TTP construct, the tactics level is where the education and experience of the Leaders becomes critical. While home-station training already provides the bulk of the incoming knowledge, it is still largely limited to field problems. Time and resources generally limit the scope of home-station training events and this challenges the development of the organizational processes and procedures, especially in the areas of long-term data management. The institutional training must enable Leaders before they

## Enabling Army Digital Organizations

arrive at the unit, as they are responsible for providing the vision, command climate, and training that will foster an effective digital organization.

### Digital Environments

A critical example is preparing Leaders to design and resource their own field problems focused on fully exercising a digital organization. These events require more preparation and a different approach than those focused on traditional movement and maneuver combat tasks. The largest obstacle by far is the establishment of the external actors, stimuli, and data sets needed to establish and fine-tune the Processing, Exploitation, and Dissemination (PED) of data between the organization and other units. Not understanding or replicating the “digital environment” may result in Leaders overlooking critical gaps or establishing unnecessary or duplicate processes and procedures.

Current training incorporates similar frameworks; however, the critical aspect is maintaining focus on the terminal learning objectives oriented toward understanding the digital capabilities, limitations, and interactions rather than the procedures of operation. Therefore, the challenge of realistic digital Leader training becomes generating an appropriate digital environment. The environment needs enough “player” elements to generate a realistic amount of data and human communications.

Simulations can [mostly] represent and generate the data, but not the human element. This is the weakest area of most digital exercises, the lack of enough external actors to fully stimulate the training audience. In addition, where a branch’s duties rely heavily on interacting with other branches or functions, the exercise will require experienced subordinate or peer elements with those skills. Thus, resourcing the equipment and appropriate role-players, military or contract, for two levels up and one level down for multiple training echelons at every schoolhouse becomes untenable.

A method to generate these environments, without creating twelve duplicate brigade-battalion-company facilities, might leverage a dedicated secure network between the installations similar to the Battle-Lab Collaborative Simulation Environment (BLCSE). This would require synchronization in the training schedules, but would allow for multiple Basic Officer Leader Course (BOLC) and Captains’ Career Course (CCC) classes to replicate company and battalion level elements at different locations under a single brigade role-player resource. For some classes, there may be an opportunity to incorporate Intermediate Level Education (ILE) classes or even War College classes as brigade, division, or corps staffs. Such a set-up would also allow consolidating the respective branch “expert” role-players at their schoolhouse, as well as simulating and varying digital conditions such as bandwidth, latency, or intermittent connections in addition to the physical time zone and distance.

The actual degradation or failure of one or more links between these systems would generally top the list as one of the major drawbacks, however that really only applies for procedural training programs. Network links really go down and operations really continue; the appropriate response would be to include the students in the trouble-shooting, rather than isolating them from it – as field commanders will expect them to understand the implications, adapt their procedures or switch processes to accommodate, and report communications status as they continue operations.

## Enabling Army Digital Organizations

This ability to understand the architecture sufficiently to tailor it to missions, styles, and objectives and maintain current operations and future planning under degraded and intermittent conditions is the reality that leader digital education should address. Leaders who are not fully enabled and cognizant of the capabilities and limitations of the digital systems and data exchanges will miss opportunities to exploit the available capabilities during training, and consequently deployment. This limits their capacity to build more effective and efficient processes and procedures and to take advantage of new processing, visualization, and collaboration technologies.

### Home-Station Training

The next piece is to track and plan for these skills within the formation. Within the previous analogy, this is comparable to weapons qualification, and in some sections, the importance may even rise to the crew qualification level. However, due to the interdependency of the systems, designating and tracking the training and competency of digital skills could become more complex than individual marksmanship. Thus, it is more akin to collective training, and the Army should derive effectiveness measures at the unit level rather than the individual.

Continuing the marksmanship analogy along into home-station training, the Army should establish a select few processes and procedures into "digital tables." Notwithstanding the goal of enabled, innovative Soldiers and Leaders, there are certain processes and procedures that must be common across peer elements to ensure the higher elements can operate efficiently and effectively.

Standardizing these into battle-drills and tables would begin to build out a common core competency across organizations and reduce friction between organizations in collaborative command and control situations. These digital tables can easily be incorporated into the current Mission Support Training Facility (MSTF) structure.

### How do we enable administrators?

Unfortunately, the individual marksmanship analogy does not necessarily apply to the unit's administrators. These Soldiers are more like master gunners or an operations and range cadre. While individuals can pick up and adjust at their own pace, the administration of the network (permissions, naming, settings, etc.) is more like scheduling, coordinating, and running a range than marksmanship with a weapon. The impact on unit operations is similar: previous experience and doctrinal publications will carry the administrators through the basic needs (albeit slower and less efficiently), but a lack of currency on the latest constraints (things you must do), restraints (things you must not do), and regulations may cause some undesired turbulence.

Just like range and ammunition duties, these administration duties require administrators to have credentials, certifications, and authorizations.

These ever changing constraints, restraints, and regulations for Information Assurance (IA)<sup>3</sup> (integrity, confidentiality, availability, authentication, verification, protection, and non-repudiation) and the resulting complexity of the administration tasks impose a much greater challenge than adapting to a new version of a battle-command system application. The units cannot effectively train their

## Enabling Army Digital Organizations

administrators off-line on a set of static tasks when the latest Information Assurance Vulnerability Alert (IAVA) has the potential to completely change the administrative procedures or have significant implications to other established unit processes and procedures.

Maintaining this vigorous defense against digital attacks requires constant vigilance and strict attention to detail. This, in effect, almost requires administrators to administer a functioning system routinely in order to maintain the currency and skills necessary in these areas. In order to provide the hands-on experience to administrators (and to train users), several units have attempted to establish their tactical networks in the garrison environment, only to encounter steep challenges and roadblocks. Without venturing to address the multitude of specific arguments against this in detail, the basis for the collective argument is specious. The argument generally presents a compelling picture involving vulnerabilities caused by granting the certifications, authorities, and privileges required by the systems and administrators to function; however, these are the same systems and administrators the deployed unit will depend on to assure connectivity and enforce security with real-world data and consequences.

Accomplishing the training and currency goals for the administrators does not require that every single battle command system operate constantly on the network. The unit could meet most of the need by simply establishing the Microsoft Exchange Server™, Microsoft Office SharePoint Server (MOSS)™, Adobe Connect structures, and administering the unit's user accounts. Unfortunately, these are the exact systems affected by the "consolidation of servers" constraint prescribed in paragraph 6-2.d. of Army Regulation 25-1<sup>4</sup>.

### Distributed versus Consolidated

Aside from the limiting effect on the experience level and currency of unit administrators, the server consolidation requirement has implications on tactical operations if it expands into that arena. While the requirement, carried over from business practices, was clearly an adoptable and cost-saving strategy in garrison, it is in direct competition with the distributed nature of tactical operations. Optimizing the network and services architecture is a delicate balancing of enterprise capabilities and efficiencies with the responsiveness of local servers and the constraints of connectivity and bandwidth. While there are multiple arguments for both sides (in addition to those just mentioned), suffice it to state that the goal of both sides is to provide the most secure, responsive, and flexible solution with the least resource burden deployed out to the end user. However, the natural tendency is to copy success and re-build what you have worked with before, so there should be appropriate caution that any consolidation of services in tactical environments is accomplished to enhance operations and not simply due to "business efficiencies" or misinterpreting "enterprise management" as [enterprise consolidation].

Extending the business practice of consolidation of servers to the tactical network is comparable to trending away from Mission Command and toward Detailed Command complete with all of the drawbacks inherent in that style of leadership.

*"... Detailed command stems from the belief that success in battle comes from imposing order and certainty on the battlefield. A commander who practices detailed command seeks to accomplish this by creating a powerful, efficient C<sup>2</sup> system able to*

## Enabling Army Digital Organizations

*process huge amounts of information, and by attempting to reduce nearly all unknowns to certainty. Detailed command centralizes information and decisionmaking authority. ...” Para 1-65 FM 6-0*

*“... Detailed command is ill-suited to taking advantage of rapidly changing situations. It does not work well when the communications and information flow is disrupted. It inhibits the judgment, creativity, and initiative required for success in fluid military operations. Because of these disadvantages, mission command is a better C<sup>2</sup> concept in almost all cases.” Para 1-66 FM 6-0*

This highlights the main drawback to consolidation of servers (and really, any consolidated enterprise system) is that they generally require ubiquitous and robust interconnections to provide the real advantages, which is sometimes a challenge in the current and future deployed environments. Consolidating SharePoint and other data storage and management systems at higher [off-site] levels effectively multiplies the units’ dependence on these links, and cripples their operations when the links are down or while moving into new positions while the links are being re-established. The connectivity and bandwidth challenges are not going to go away in Afghanistan and are present in other mountainous or undeveloped regions where the Army is likely to deploy. While the Army is applying a large effort toward providing ubiquitous and robust interconnections (and technology advances will drastically change the optimal solution), designing operations by building dependence into the plan is arguably exactly the wrong approach.

There are also recent examples where the best solution for now, is not the best solution for next year. Currently, the commercial IT community has begun to examine “physicalization” in response to the previous rush to virtualization. Simplistically, virtualization came about to better utilize the processing capacity of high-end servers, while still segregating services on multiple individual virtual machines for security and availability (the compromise or crash of one service does not affect the others). So, one high-end physical machine actually contains multiple virtual machines, each with specific services or data, and the physical machine is run at maximum capacity. In contrast, physicalization is an attempt to employ multiple low end (and sometimes cheaper) physical machines to reduce the power and cooling costs within large datacenters while maintaining the isolation of services. So, the same number of services are now installed on individual (or clustered) low-end machines which still minimizes wasted processing capacity, but require much lower power and cooling resources.

The Army routinely conducts policy reviews as technology progresses, but it should similarly focus on revalidating the operational and tactical considerations first and only then examine which enterprise policies and standing operating procedures best support these needs. Arguably, physicalization’s focus on “Good Enough” combined with lowering the power and cooling requirements is a better fit for the deployed Army than consolidation and virtualization’s focus on enterprise security and availability objectives.

These re-assessments should occur hand in hand with the commoditization of previously specialized hardware and the integration of previously separate handcrafted software and solutions into interoperable and enterprise platforms and solutions.

### How do we enable innovation?

The commoditization of hardware and integration of software has led the Army Battle Command Systems to move increasingly toward standardization on the Microsoft Windows platform, with minor exceptions employing UNIX as a foundation. The move to standard and uniform platforms and interface concepts is a positive and necessary condition, although it poses a risk of reliance on a single architecture and resulting influences on *how things are done*. However, the “Open Source” movement and some accompanying UNIX concepts have mitigated some of the limitations of single source dependency through influencing the development of abstracted programming languages such as Visual Basic and Python. These high level scripting and programming languages combined with more “human readable” data exchange standards such as eXtensible Markup Language (XML)<sup>5</sup> and JavaScript Object Notation (JSON)<sup>6</sup> have made Google Earth™ and even aspects of My Space™, Facebook™, and other such social networking sites a training environment for accomplishing similar customization and automation tasks in deployed units. When the “popular” teenagers, and not just the computer-inclined, are writing scripts to enhance their social networking pages - then these sorts of skills are poised to become much more prevalent within the ranks.

These skills are directly translatable to any information exchange environment that enables safe local access to battle command system and server data through a web API or a client application. Although designed for developers and not specifically for local client access, the PASS Client Interface is an example of such an application. This application provides a robust, accredited, and tested interface to the PASS, such that any script or code written to manipulate the ABCS data is buffered from direct interaction with the battle command systems. Some adjustments to this interface design could provide simpler and easier access to the data to enable any user to query and process data locally without affecting the battle command systems or having to maintain pace with ABCS design standards and configurations.

Once the data is easily available to users familiar with scripting and high level scripting languages in a format designed for easy manipulation, they can transform the data to other formats or standards more easily. This allows them the flexibility to use other visualization or data processing applications without needing extensive coding or developer support. This is where innovation begins.

### Non-Standard Solutions

The trade-off that the Army must monitor in the institutional sense is the difference between enabling and encouraging innovation and reining in the “Wild Wild West” by maintaining consistency and reducing time and effort spent on divergent solutions. The current strategy for mitigating these issues (consciously or unconsciously) relies heavily on the Field Service Representatives who establish, support, and maintain the systems in the field. A digital organization enabled by Soldiers and Leaders proficient in Information and Knowledge Management should execute most of these functions as a matter of course, without needing augmentation for fielded programs and systems. By its very nature, the innovation side of information technology is and probably will continue to be a “contractor’s playground,” but those efforts should be focused on developing and refining new processing methods and visualization tools, not constantly reengineering the connections between applications and systems.

## Enabling Army Digital Organizations

The Army has historically developed a set of requirements for a new system, which include the Interface Control Document (ICD). Incorporating this into multiple formal program requirements presents an increased opportunity for disconnected decisions. For example, as an authoritative data source for some information, the ICD for system “A” includes a requirement to catalog and publish data to systems “B”, “C”, etc. in a specific format on a specific schedule. The recipient systems then have requirements to ingest this data. When system A encounters a need to change that impacts the publishing requirements, all of the other systems’ requirements must be examined and addressed. Ideally, this is just a bit of added program coordination, but differing program schedules and objectives have created situations where progress forward on System A is stalled because system B is heavily reliant on the old requirement and cannot change in sync.

The ABCS developers have been dealing with these information exchange issues and requirements adjustments for some time; the concepts espoused below are already present in the guidance for Army Net-Centric Data Management Program (ANCDMP)<sup>7</sup> and the Joint Technical Architecture–Army (JTA–A)<sup>8</sup>. The requirements include Data Performance Plans (DPP)<sup>9</sup>, Authoritative Data Sources (ADS)<sup>10</sup>, Information Exchange Standards Specifications (IESS)<sup>11</sup>, and eXtensible Markup Language (XML). However, currently fielded systems generally remain focused at the “message” level, and not the “data element” level. The Army should apply more attention to developing a uniform information exchange architecture based on configurable data requests. An ideal architecture would enable a new system to interoperate with the other systems through communicating three components: standard data exchange primitives, authentication protocols, and formats tiered by bandwidth.

Data based standards should be built on common “primitives” which generally imply that the display of the data is divorced from the storage of the data. An example is date/time in Microsoft Excel™, which internally stores every date or time as the number (and fraction) of days starting from January 1, 1900 as “1” (the 5/2 ID (SBCT) deployed around day 40,000 or July 6, 2009). The Ground Positioning Sensor (GPS) suite contains another such method, with the epoch for the GPS Week Number “0” starting on January 6, 1980. In both of these systems, the display of information is separate from the storing and processing of information. The utility of this is immediately obvious to anyone who has dealt with coordinates, which have a huge number of standards and formats (43.245216, -96.582449; 43 14.713N, 96 34.947W; 431442.78N 0963456.82W, 43° 14’ 42.78” N, 096° 34’ 56.82” W; 14T 696269 4790884; 14TPN9626990884; 14T PN 962 908; 14T PN 9626 9088; etc.). Most of these formats are already well defined and generally agreed to. There should be little work to incorporate into a common data element based standard. The real change would be to enforce the transfer of data in these formats (and datums for coordinates) and requiring each system that does not natively use that format to have a conversion routine in the publishing and subscribing components.

Moving from message-based standards to data element based standards would also require each system to contain publishing and subscribing routines that are slightly more complex in order to dynamically determine the data to request and publish for each exchange. However, this is not an exclusive proposition, as the previous formats could remain for messages that feed time-critical processes or embedded or other systems with low processing power. By moving to the data element in the information exchange standards, changes in data exchanges between systems can occur without



## Enabling Army Digital Organizations

having to address a multitude of other systems' designs. For example, if a new field is required between an authoritative data source and a subscriber, the subscriber simply adds the field to those specific requests through flexible parsers, while other systems only request the previously "standard" fields. Note the importance of identifying the authoritative source for the data; as systems collect, combine, and exchange information the data can become "stale" and systems should be able to request the data from a single authoritative source at each level.

These authoritative data sources should also have well defined authentication protocols to control access to information. Regardless of the determination of which systems or users have access to which data, the protocols should allow for authenticating an anonymous request (open to any requestor), an externally validated request (e.g. Active Directory, groups, smartcard), and a specifically authorized request (an administrator authorizes specific machines or users on the source itself). Likewise, the actual technical implementation of the mechanisms is less important than establishing clear and common means for accomplishing the three types of authentication.

Similarly, the format of the exchanges should be tiered along bandwidth and usability. Time sensitive and mission critical systems should have the smallest possible format to speed transmission and allow for restricted bandwidth. At the other end, a fully documented human readable format (such as XML with expressive tag names) should be employed for Soldiers and developers who wish to have the information in human-readable and flexible formats - for easy transformation or export into other data processing or visualization tools. The mid-tier should be something that balances both ideals, more compact than fully tagged XML, but more readable and easier to manipulate in scripts than binary or fixed column text.

### Local versus Global

Once the data exchange foundations are developed and implemented (in whatever fashion, not limited by the previous discussion), the standardization of tags, labels, terms, and definitions is the final requirement.

Historically, while doctrine is the basis for operations, commanders have had broad latitude to adopt local Standing Operating Procedures and terminology ("Green-Green," "Blue-26 Report," etc.). Two main factors enabled this practice: the amount and type of data exchanged and how much of the reported data was actually used.

The increase in Command and Control and ISR capability comes with increased data exchange requirements. Likewise, these capabilities come with an increase in digitally connected systems. These changes greatly affect the "local" nature of these conventions, as it changes the interdependence and interactions between peer and subordinate units. Previously, while units operated in a combined fashion, their internal conventions largely remained internal to the unit; and the differences could be translated by the staff for external consumption. Under an ever-increasing load of data and information exchange, the staff will become overburdened by the effort to adjust local conventions into the next higher element's local conventions.



## Enabling Army Digital Organizations

In some cases, previous standards that were not digitally critical, and therefore subject to local convention, suddenly become critical when a new system is placed into operation. Some examples are setting the master-net time on various radio systems, or certain settings within the Forward Observer System (FOS) when used with the Non-Line-of-Sight Launch System (NLOS-LS) prototypes.

## Conclusion

The interdependence between the education and experience of Soldiers and Leaders and the flexibility of the supporting architecture requires careful consideration as the Army forms, trains, and deploys formations in the digital era. Soldiers and Leaders must arrive at the forming unit fully prepared: a master of procedures; adept at various techniques; and well versed in the capabilities, interactions, and most importantly the purposes behind the Army Battle Command Systems or any digital infrastructure the Army adopts. Ensuring the institutional training provides a much deeper understanding of data Processing, Exploitation, and Dissemination (PED) and a solid foundation in the interactions between digital data and battle command systems will better enable the Soldiers to employ the systems and the Leaders to develop, shape, and structure the unit into an effective digital organization.

---

<sup>1</sup> Paragraph 11–1 of *How the Army Runs: A Senior Leader Reference Handbook, 2005-2006*, describes the Department of Defense (DOD) and U.S. Army management system used for the research, development, and acquisition (RDA) of materiel systems as “a combination of structure, process, and culture.

- Structure is the sum of the guidance provided by law, policy, regulation or objective, and the organization provided to accomplish the RDA function.
- Process is the interaction of the structure in producing the output.
- Culture is the cumulative sum of past practices and their impact on interpretation of guidance and attitude toward institutional changes to the system.”

<sup>2</sup> Paragraph 16–1.c. of *How the Army Runs: A Senior Leader Reference Handbook, 2005-2006*, describes Army Knowledge Management (AKM) as “the comprehensive strategy to transform the Army into a net-centric, knowledge-based force. The strategy consists of a robust set of goals and objectives, which once achieved, will improve the decision dominance of our tactical commanders and our business stewards. These goals and objectives concentrate on managing the information technology (IT) infrastructure as an Enterprise in line with the Global Information Grid (GIG), with a view toward reducing the resource and equipment footprint and creating ubiquitous access through AKO as the Enterprise portal to knowledge centers, functional applications and network services. The use of best business and governance practices and the emphasis on innovative human capital strategies are key goals of AKM.”

<sup>3</sup> IA seeks to maintain effective command and control of friendly forces by protecting critical information infrastructures from unauthorized users, detecting attempts to obtain or alter information, and reacting to unauthorized attempts to obtain access to or change information. These measures focus on the integrity, confidentiality, availability, authentication, verification, protection, and non-repudiation of the infrastructures and the information contained within. AR 25–1

<sup>4</sup> 6–2.d. Consolidation of servers. DOIMs on each post will consolidate servers for Army tenants residing on the post within the installation data center or designated server farm locations. Tenants associated with other Army networks that encompass multiple posts may remain within their networks until such time as Army migration efforts are complete. Army tenants on each post will assist the DOIM in consolidating servers to locations specified by the DOIM. AR 25–1

<sup>5</sup> XML is a tagging language used to describe and annotate data so it can be consumed by human and system interactions. It is typically arranged hierarchically using elements and attributes. It also uses semantically rich labels to describe elements and attributes to enable meaningful comprehension. AR 25–1

<sup>6</sup> JSON is a format used to structure data in text format so object-oriented programming languages (and scripts) can directly consume a complete object without having to reestablish the object's structure. The notation is not labeled as expressively as XML, but retains the object's structure in a manner that humans can readily examine.

<sup>7</sup> The ANCDMP establishes policy, guidance, and instruction about the set of data standards, business rules, and data models required to govern the definition, production, storage, ownership, and replication of data. AR 25-1

<sup>8</sup> The JTA-A is a complete set of rules derived from the Joint Technical Architecture that prescribe the technical standards for Army IT systems and enable interoperability among joint systems. AR 25-1

<sup>9</sup> The DPP is an organized and structured approach to the specification and collection of enterprise artifacts in support of community of interest (COI) objectives that operate in a common and shared fashion. Data performance planning collects, develops, and maintains these artifacts and is of primary interest to information system professionals charged with ensuring that information systems meet the needs of the COI. These artifacts are often referred to as "metadata." AR 25-1

<sup>10</sup> An ADS is a source for a data structure and value domain set that is readily available to provide common domains of data values to different databases. AR 25-1

<sup>11</sup> An IESS is a narrowly scoped data model to facilitate data exchange and interoperability between communities of interest. AR 25-1